Statement of Commissioner Melissa Holyoak,

Joined by Commissioner Andrew Ferguson

Health Breach Notification Rule

File No. P205405

April 26, 2024

The Health Breach Notification Rule ("Final Rule") that the Commission adopts today exceeds the Commission's statutory authority, puts companies at risk of perpetual non-compliance, and opens the Commission to legal challenge that could undermine its institutional integrity. I share the majority's goal of protecting the privacy and security of consumers' identifiable health information,[1] and I support vigorous enforcement of laws protecting sensitive personal information with which Congress has entrusted the FTC.[2] I would support finalizing a rule that extends and clarifies the scope of the Commission's enforcement in this important area of consumer protection if that rule were consistent with our grant of authority from Congress. But, no matter how the majority attempts to shoehorn its desired policy goal into a "plain reading" of the statute,[3] I cannot support a rule that exceeds the bounds Congress clearly established. Indeed, a core principle guiding my tenure at the Commission will be that our rules must effectuate the law as it is—not as the Commission may wish it to be. For these reasons, I respectfully dissent.

The American Recovery and Reinvestment Act of 2009 ("Recovery Act")[4] authorized the Commission to issue a rule requiring vendors of "personal health records" ("PHRs") and related entities that are not covered by HIPAA to notify individuals and the FTC of a "breach of security" of "unsecured PHR identifiable health information."[5] The Commission issued the Health Breach Notification Rule in 2009,[6] initiated a routine review of the Rule in 2020,[7] issued

[1] Like the majority, and other Commissioners before me, I support federal privacy legislation, particularly where such legislation could address gaps in sector-specific laws and level the playing field for companies navigating a patchwork of laws. And like the majority, and other Commissioners before me, I care deeply about protecting the privacy and security of consumers' health information, particularly where it falls outside the bounds of the Health Insurance Portability and Accountability Act ("HIPAA"). For more than two decades, the FTC has been in a leader in protecting consumers' health information. *See, e.g.*, *Eli Lilly*, FTC File No. 0123214 (May 10, 2002), https://www.ftc.gov/legal-library/browse/cases-proceedings/012-3214-eli-lilly-company-matter. I look forward to continuing the Commission's important work in this area.

[2] *See, e.g.*, Children's Online Privacy Protection Rule, 16 CFR Part 312, as authorized by the Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 *et seq*.

[3] Joint Statement of Chair Lina M. Khan, Comm'r Rebecca Kelly Slaughter, and Comm'r Alvaro M. Bedoya at 2 (Apr. 24, 2024) ("Majority Statement").

[4] Am. Recovery and Reinvestment Act of 2009, Pub. L. 111-5, 123 Stat. 115 (2009).

[5] 42 U.S.C. § 17937(a), (g).

[6] 74 Fed. Reg. 42962 (Aug. 25, 2009).

[7] 85 Fed. Reg. 31085 (May 22, 2020).

a policy statement re-interpreting the then-current Rule in 2021 ("2021 Policy Statement"),[8] issued a Notice of Proposed Rulemaking on June 9, 2023 ("NPRM"),[9] and today issues the Final Rule.[10]

I am encouraged that today the Commission is acting by rulemaking, as authorized by statute and following a period of notice and comment that elicited a range of views, rather than acting by fiat in a policy statement, as the Commission did in 2021.[11] I cannot endorse any policy statement that either displaces Congress's authority to make law or subverts the rulemaking process. The 2021 Policy Statement did both. The majority clearly recognizes this overreach. After all, if the 2021 Policy Statement had any force, today's rulemaking would be unnecessary.

Setting aside this troubling history, I turn to the Final Rule itself, which, unfortunately, I find equally troubling in its extension beyond the parameters established by Congress.

Some background first. Under the Recovery Act, PHR identifiable health information means "individually identifiable health information," as defined by the Social Security Act, 42 U.S.C. § 1320d(6).[12] The Social Security Act defines "individually identifiable health information" as information that is "created or received by a health care provider, health plan, employer, or health care clearinghouse."[13] The Social Security Act then defines "health care provider" to include three categories: "[1] a provider of services (as defined in 1395x(u) of this title), [2] a provider of medical or other health services (as defined in section 1395x(s) of this title), and [3] any other person furnishing health care services or supplies."[14]

The Commission takes liberties with the final category in that definition ("any other person furnishing health care services or supplies") to adopt a new, capacious definition of "covered health care provider" and a new, similarly capacious definition of "health care services and supplies," whose joint effect is to sweep a large swath of apps and app developers under the purview of the Final Rule. These expansive definitions are not consistent with the statute. Under longstanding principles of statutory interpretation, the final category of provider ("any other person…") must be understood in relation to the first two categories ("provider of services" and "provider of medical or other health services").[15] When a statute contains a list, "each word in

---

[8] *See* Statement of the Comm'n on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf ("2021 Policy Statement").

[9] 88 Fed. Reg. 37819 (June 9, 2023).

[10] *See* Statement of Basis and Purpose ("SBP") accompanying the Final Rule, Section I (summarizing procedural history).

[11] *See* 2021 Policy Statement, *supra* note 8.

[12] 42 U.S.C. § 17937(f)(2).

[13] 42 U.S.C. § 1320d(6).

[14] *Id.* § 1320d(3).

[15] *See Yates v. United States*, 574 U.S. 528, 549-51 (2015) (Alito, J., concurring); Antonin Scalia & Bryan A. Garner, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 195-196,199-200 (2012).

that list presumptively has a 'similar' meaning" under the canon of *noscitur a sociis*.[16] And when a general term follows a list of specific terms, the *ejusdem generis* canon teaches that the general term "should usually be read in light of those specific words to mean something 'similar.'"[17] Together, these canons instruct that the final category of health care provider that includes the general term "*other* person" must be similar to the more specific terms that precede it.

The first two categories of health care provider incorporate the definitions of Sections 1395x(u) and 1395x(s) of the Social Security Act, respectively.[18] The first category of provider includes "a hospital, critical access hospital, rural emergency hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, or…a fund."[19] The second category of provider includes an extensive list (Section 1395x(s) includes 17 paragraphs and over 35 subparagraphs) of medical professionals including physicians, physician assistants, nurse practitioners, clinical psychologists, clinical social workers, and others, and the specific services administered by medical professionals.[20] These two categories comprise traditional forms of health care providers.

The final category, addressing "any other person furnishing health care services or supplies," must therefore only include persons that are "similar in nature" to these first two categories.[21] The majority argues that my "effort to cabin the third category…reads it out of existence, violating the canon that holds interpretations giving effect to every clause of a statute are superior to those that render distinct clauses superfluous."[22] This application of the canon is incorrect. Requiring *similarity* among categories does not result in superfluity; it merely prevents interpretations that extend beyond what the text permits. A catch-all's limited application due to its context is not a reason to expand that phrase to encompass dissimilar applications.

The Final Rule's definition of "covered health care provider" is not remotely similar, because it incorporates a new, astonishingly broad definition of "health care services or supplies," which means "any online service such as a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools."[23] Thus, the Commission transforms "health care provider," which both under common usage and in context of the statutory provision means entities such as physicians and hospitals, to now include any company "furnishing" a health-related app.[24] As a

[16] *Yates*, 574 U.S. at 549.

[17] *Id.* at 550.

[18] 42 U.S.C. § 1320d(3).

[19] 42 U.S.C. § 1395x(u).

[20] *Id.* § 1395x(s).

[21] *Yates*, 574 U.S. at 545 (internal quotation marks omitted).

[22] Majority Statement at 2.

[23] Final Rule at 98.

[24] The SBP explains that an app developer (or any company "furnishing" a health app) would be covered as a health care provider because its health app is a health care service or supply. SBP at 7, 22-28.

result, the Final Rule creates a tautology: Health app developers may be "vendors of personal health records" by offering an app containing health information that has been created or received by a health care provider, where *the health app developer is itself the health care provider* that creates or receives that health information by virtue of offering the app.

Notably, even though the Department of Health and Human Services ("HHS") interprets this same provision of the Social Security Act, HHS has—notwithstanding the majority's assertion to the contrary[25]—never interpreted the term "health care provider" to reach the expansive, creative conclusion that the Commission does today.[26] The majority's argument misstates the scope and language of the HIPAA Privacy Rule, which only applies to HIPAA "covered entities" and their "business associates,"[27]—i.e., to traditional health care providers that do not include the broad swath of app developers the Final Rule will encompass. Significantly, the majority omits from its characterization of the term "health care" HHS's own illustrations of that term, which highlight the proximity to traditional forms of health care by different kinds of medical professionals:

> (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
> (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.[28]

The Majority Statement repeatedly *says* that HHS defines "health care" broadly,[29] but the language it cites provides no such support.

Aware of this incongruency, the Commission seeks to differentiate its use of "health care provider" from that of "other government agencies."[30] Yet the Commission provides no explanation *why* its definition should differ, particularly where it is unclear whether the Commission has interpretative authority over the Social Security Act's definition of health care provider and where other agencies *are* delegated such interpretative authority.[31]

The Commission also takes troubling liberties with the statute's definition of "personal health record," which are evident from a side-by-side comparison of the statute and the Final Rule:

---

[25] Majority Statement at 3.

[26] *See* NPRM at 37823.

[27] 45 CFR §§ 160.102-103.

[28] *Id.* § 160.103.

[29] Majority Statement at 3-4.

[30] SBP at 26.

[31] *Id.* at 13 (noting that HHS interprets these provisions of the Social Security Act). *Cf. City of Arlington, Tex. v. F.C.C.*, 569 U.S. 290, 323 (2013) (Roberts, C.J., dissenting) ("When presented with an agency's interpretation of such a statute, a court cannot simply ask whether the statute is one that the agency administers; the question is whether authority over the particular ambiguity at issue has been delegated to the particular agency.").

Recovery Act	Final Rule
"an electronic record of PHR identifiable health information…on an individual *that can be drawn from multiple sources* and is managed, shared, and controlled by or primarily for the individual."[32]	"an electronic record of PHR identifiable health information on an individual that has the technical capacity *to draw information from multiple sources* and that is managed, shared, and controlled by or primarily for the individual."[33]

Under the Final Rule, a PHR need not actually draw *health information* from multiple sources, as the statute contemplates (because the statutory phrase "that can be drawn" modifies its immediate antecedent, "health information"). Rather, under the Final Rule, a *single* source of health information will render an app a PHR as long as the "PHR" has the "technical capacity" to draw some *other* information elsewhere.[34] The implications of this change, in conjunction with the expansion of "health care provider," are significant. Any retailer that offers an app that tracks health-related purchases (e.g., bandages, vitamins, dandruff shampoo) may be a vendor of a PHR covered by the Rule if the app draws health information (e.g., purchasing information) from the consumer and the app has the "technical capacity" to draw *any* information from *any* other source. As the Statement of Basis and Purpose notes, commenters warned that virtually every app has the technical capacity to draw some information from more than one source.[35] That expansive scope could be appropriate if Congress's language permitted it. But the Commission's interpretation, which effectively renders the Recovery Act's "multiple sources" requirement meaningless, ignores longstanding principles of statutory interpretation that require each provision of a statute to be given effect.[36]

The Commission's expansive definitions of "covered health care provider," "health care services and supplies," and "personal health record" have a profound effect on the scope of the Rule: Most companies that offer or disseminate health-related apps or similar products would be treated as "covered health care providers" that therefore hold "PHR identifiable health information" in their apps (*i.e.*, PHRs), such that they are vendors of PHRs—even if their app is merely health-adjacent.

Remarkably, the Commission imposes no limit on this extraordinary breadth in the Rule itself. Rather, in a post-NPRM attempt to check the scope, the Commission fashions a limiting principle: Apps are covered only if they are "more than tangentially relating to health."[37] This extra-statutory, extra-regulatory limit has several significant problems.

---

[32] 42 U.S.C. § 17921(11) (emphasis added).

[33] Final Rule at 99 (emphasis added).

[34] *See* SBP at 32 ("Next, adding the phrase 'technical capacity to draw information' clarifies that a product is a personal health record if it can draw *any* information from multiple sources, even if it only draws *health* information from one source.").

[35] *See id.* at 34.

[36] Scalia & Garner, *supra* note 15 at 174 (discussing surplusage canon).

[37] SBP at 28.

First, if the majority were correct, from where would it draw the authority to impose this "more than tangentially relating to health" limitation? If Congress in fact commanded us to cover all the apps the majority claims, this extra-textual limitation would be beyond our power to impose.[38] Why, then, does the majority blink in the face of what it understands Congress to have required? There may be good policy reasons not to follow Congress's language—as the majority understands it—wherever it leads, but we do not have power to shortchange Congress's commands. That even the majority feels compelled to adopt this extra-textual limitation—again, as the majority understands the text—on the statute's reach suggests that the language probably does not mean what the majority says.

The second problem is substantive: What does this language mean? When does an app cross the line between tangentially related to health and more than tangentially related? If a gas station with a loyalty app sells Advil, is the app only tangentially related to health and outside the Final Rule's purview? If the gas station adds Robitussin and pregnancy tests to its inventory, does it cross the line to more than tangentially related to health? If a clothing store with an e-commerce app sells a handful of maternity shirts, is the app only tangentially related to health? If the store adds more maternity clothes, nursing bras, and some anti-nausea ginger tea to its in-app offerings, is the app more than tangentially related to health? If vitamins, over-the-counter medicines, acne creams, bandages, and similar items comprise 0.1% or 1% or 10% of a superstore's inventory, when is the retailer's e-commerce app more than tangentially related to health? I see no clear answers to any of these hypotheticals in today's Final Rule, which suggests that the marketplace will see no clear answers either.[39]

The third problem is procedural. The Commission did not propose this ambiguous but impactful limitation in a Notice of Proposed Rulemaking—likely because there is no statutory basis for this newly-created language. Rather, it introduces this crucial concept for the first time in a Statement of Basis and Purpose (a purely interpretive document) as a *post hoc* fix to the problem the Commission itself created with its expansive definitions. As a result, the Commission did not provide notice or receive public comment on the efficacy or propriety of this limitation, depriving the public of its opportunity to meaningfully participate in the rulemaking process and depriving itself of potentially valuable input from commenters.

The final problem is that this *post hoc*, extra-regulatory limitation renders the Commission's burden analysis inadequate. The Paperwork Reduction Act ("PRA") requires the Commission to estimate the reportable breaches by entities covered by the Rule and compliance costs.[40] The Regulatory Flexibility Act ("RFA") requires the Commission to assess the economic

---

[38] *See Nat'l Fed'n of Indep. Business v. Dep't of Labor*, 595 U.S. 109, 117 (2022) (per curiam) ("Administrative agencies are creatures of statute. They accordingly possess only the authority that Congress has provided.").

[39] The expansive coverage increases the likelihood of creating unintended consequences. Will the gas station decline to add over-the-counter medicines to its inventory to avoid crossing the line of "more than tangentially related to health"? Will the clothing retailer shy away from maternity apparel? Will the e-commerce giant avoid selling bandages and dandruff shampoo? These potentially detrimental outcomes undermine a Rule intended to benefit consumers.

[40] *See generally* 44 U.S.C. § 3501 *et seq.*; SBP at 86.

impact on small businesses.[41] Apparently relying on the SBP's "more than tangentially related to health" limitation, the PRA and RFA analyses only address breaches by apps categorized as "Health and Fitness."[42] Because the Rule itself contains no such limitation, general retailers with e-commerce apps, gas stations with loyalty apps, and other similar generalists that sell any health-related items do not factor into these analyses. As a result, they likely dramatically underestimate the numbers of regulated entities, number of breaches, and costs to businesses.

Perhaps the breath of the Final Rule would be more of a theoretical than practical concern to businesses, if they could adopt practices sufficient to avoid any breach that would trigger notice obligations under the Final Rule, or, in the event of a breach, err on the side of notification. But Section 318.3(b) of the Final Rule imposes affirmative obligations on companies to notify their service providers if they are covered by the Final Rule, regardless of whether they experience a breach.[43] To comply with this requirement, companies must know whether they are covered by the Rule—that is, which side of "more than tangentially relating to health" they fall on. Without clarity on that line, companies run the risk of being in perpetual violation of the Final Rule and, therefore, perpetually at the mercy of the Commission's enforcement discretion. The Commission, at this moment, may not intend to pursue such technical violations. But any expression of intended restraint will be cold comfort to companies that have seen the Commission's self-imposed restraint wax and wane in other areas.[44]

I find the majority's liberties with the statute particularly troubling because they are unnecessary to reach health apps. Indeed, the Commission's own recent enforcement action against digital healthcare platform GoodRx makes that clear. Only last year, a bipartisan Commission applied the 2009 Rule to GoodRx's online platform and app because the company received identifiable health information on prescription medications (among other things) from pharmacy benefit managers and pharmacies, among other sources, so that consumers could manage their information.[45] The majority argues that today's changes are necessary to provide clarity to the market about the Rule's scope,[46] but *GoodRx* has already done that—and I would support changes to the Rule that are consistent with the statute. In short, I agree with the majority's goals—safeguarding consumers' sensitive health information and implementing a Congressional mandate to put consumers on notice of the breach of that data—but I believe that we must effectuate those goals within the scope of the law as it is, rather than legislating in the guise of applying the law.

---

[41] 5 U.S.C. §§ 601-612.

[42] SBP at 86, 93.

[43] This may have been a sensible requirement in 2009, when the scope of the Rule was much narrower, but it has dramatic consequences in this much-expanded Rule.

[44] Significantly, the Majority Statement is silent as to the propriety and consequences of its "tangentially related" limiting principle, likely because this approach is indefensible.

[45] *See Concurring Statement of Commissioner Christine S. Wilson, GoodRx*, Matter No. 2023090 1 n.2 (Feb. 1, 2023) ("GoodRx has violated the HBNR based on a plain reading of the text, setting aside any gloss the Commission sought to add in its September 2021 Statement on Breaches by Health Apps and Other Connected Devices."), https://www.ftc.gov/system/files/ftc_gov/pdf/2023090_goodrx_final_concurring_statement_wilson.pdf.

[46] Majority Statement at 5.

The FTC is a venerable institution that does vital work to protect consumers and promote competition, thanks to its hardworking and devoted career staff. I commend the staff attorneys, economists, and technologists who worked on the rule for their careful and thoughtful consideration of difficult issues. Ultimately, while I am sympathetic to the majority's *goal*, I fear that adopting a Final Rule that is irreconcilable with the statute and that puts companies in an untenable position puts the Commission at risk. Legal challenges may undermine the Commission's institutional integrity, and Congress may be reluctant to trust the Commission with other authority—even the much-needed authority to protect the privacy of consumers' sensitive personal information. I therefore respectfully dissent.